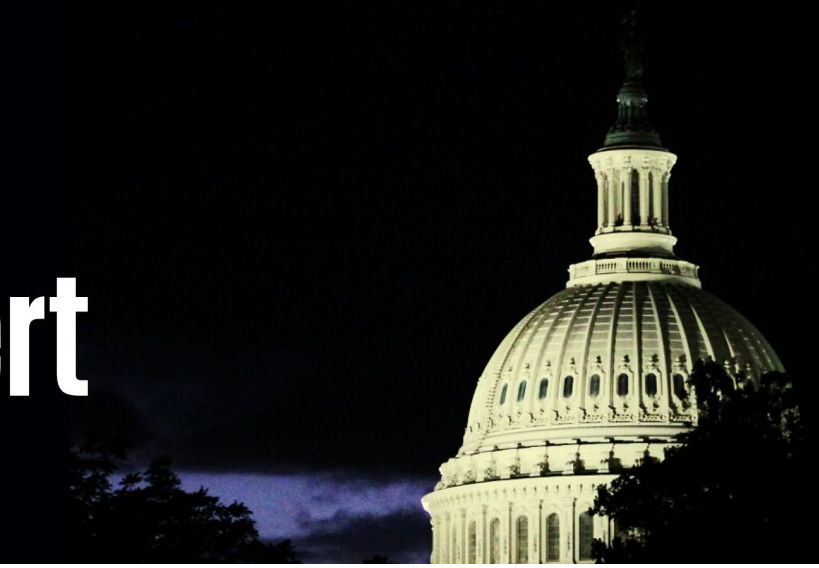
KPMG

Regulatory Alert

Regulatory Insights



February 2023

Focus on Tech: Cloud, AI, Personal Data

KPMG Regulatory Insight:

- *Regulators will increasingly scrutinize technology innovations (e.g., cloud, AI) against a company's sound risk management policies.*
- *The principle of "protecting the consumer/customer" will be expected of all industries—with a continued focus on the technology sector (e.g., children's protections, advertising) and financial services (e.g., data governance, AI bias).*
- *Companies should expect heightened expectations (and so quickly look to enhance) such areas as:*
  - *Modern technology risk management, technology resiliency and operational resiliency*
  - *Risk management and governance, data collection and privacy (see 2023 Regulatory Challenges: Technology and Resiliency; Data and Cybersecurity)*

While recognizing the many benefits to be derived from new technologies, the Administration is looking to address the challenges across sectors and the potential harms to consumers that may be realized from rapid technology development and innovation. Key issues include transparency, accountability, and privacy—as recently featured in the:

- Calls for bi-partisan legislation outlined in the State of the Union Address
- Treasury report on the Financial Services Sector's Adoption of Cloud Services
- White House Blueprint for an AI Bill of Rights

State of the Union Address

In remarks prepared for the State of the Union Address, President Biden called for Congress to pass bipartisan legislation to "stop Big Tech from collecting personal data on kids and teenagers online, ban targeted advertising to children, and impose stricter limits on the personal data these companies collect on all of us." He also called for legislation to strengthen antitrust enforcement and regulate competition among big online platforms.

Treasury Cloud Report

The Department of the Treasury's report on the adoption of cloud services in the financial services sector acknowledges an increasing trend toward cloud adoption by all types and sizes of financial institutions (FIs). Treasury suggests this trend has accelerated most recently by "customer demand for innovative offerings through digital channels and financial institution demand to accommodate remote work." It adds that models of adoption vary across the sector and that there is a wide range of service uses (e.g., IT and cybersecurity management, data storage, and computing facilities needed for artificial intelligence/machine learning applications (AI/ML)).

The report identifies several challenges associated with this broad cloud adoption, noting that the challenges cut across multiple use cases, Cloud Service Providers (CSPs), and FIs. As outlined by Treasury, the six challenges include:

- *Gaps in available talent and tools to securely deploy cloud services*, where Treasury finds the current talent pool is "well below demand," presenting potential barriers to entry for some FIs and increased risk of "misconfiguration".
- *Exposure to potential operational incidents*, such as cyber incidents, that may impact multiple regions, CSPs, or FIs as

well as technical vulnerabilities (e.g., uneven maturity of organizations or technologies) and physical events (e.g., power outages).

— *Insufficient transparency from CSPs to support due diligence and monitoring by FIs*, including information on risks related to incidents and outages needed to build technology architecture with appropriate consumer protections.

— *Potential impact of market concentration in cloud service offerings on the sector's resilience*, noting growth primarily in the adoption of services provided by three major ("Big Tech") companies as well as a lack of data needed to assess how an incident at one CSP could affect the sector.

— *Dynamics in contract negotiation given market concentration*, potentially providing CSPs with negotiating advantages especially with regard to smaller FIs and FIs with smaller scale service contracts.

— *International landscape and regulatory fragmentation*, making it difficult for U.S. FIs to adopt cloud consistently at a global scale, increasing operational and data privacy risks.

Anticipating continued and accelerated adoption of cloud services across the sector, Treasury lays out plans to engage with U.S. financial regulators, the private sector, and international partners to address the identified challenges, including:

— Establishing an interagency Cloud Services Steering Group

— Conducting follow-on work to the April 2022 "tabletop exercise" involving CSPs and the financial sector

— Progressing collaboration on the challenge areas and developing options or approaches with respect to: common definitions and terms across the sector (e.g., "critical" services); sector-wide measurement of the concentration of critical uses of cloud services and similar third-party services; incident response and communications updates among financial regulators, CSPs, and FIs; and enhancements to regulatory guidance on risk management practices for cloud services.

Blueprint for an AI Bill of Rights

The Administration released its Blueprint for an AI Bill of Rights in the fall of 2022, stating that "the use of technology, data, and automated systems in ways that threaten the rights of the American public" is "among the great challenges posed to democracy today." The Blueprint identifies five principles that the Administration suggests should guide the design, use, and deployment of automated systems to protect the public "in the age of artificial intelligence." These principles include:

— *Safe and effective systems*, that meet their intended use and contain protections from unintended use, including inappropriate or irrelevant data use.

— *Algorithmic discrimination protections*, built into systems as continuous measures to mitigate disparate treatment or impacts to people, with ongoing testing and oversight.

— *Data privacy*, where data collection conforms to "reasonable expectations" and only data necessary for the specific context is collected; consumers' permission should be sought for collection, use, access, transfer, and deletion of their data to the greatest extent possible.

— *Notice and explanation*, in plain language regarding how an automated system is being used and it how it contributed to determining an outcome impacting the consumer.

— *Human alternatives, consideration, and fallback*, providing opportunity to opt-out from an automated system, where appropriate, as well as providing a remedy to errors or to contest an impact.

The Blueprint states "automated systems should be developed with consultation from diverse communities, stakeholders, and domain experts to identify concerns, risks, and potential impacts of the system". Furthermore, to demonstrate that these systems are safe and effective, they should undergo pre-deployment testing, risk identification and mitigation, and ongoing monitoring.

The Administration highlights specific examples of regulatory actions across multiple sectors supportive of the Blueprint, including the Federal Trade Commission's ANPR on commercial surveillance, and the Consumer Financial Protection Bureau's Circular 2022-03 (Adverse action notification requirements in connection with credit decisions based on complex algorithms).

Relevant KPMG Thought Leadership:

— KPMG Regulatory Insights POV| Regulatory Scrutiny of Technology and Data

— KPMG Regulatory Alert| Data Retention and Deletion: Increasing Regulatory Expectations

— KPMG Regulatory Alert| Regulatory Focus on Cloud Computing

For more information, please contact Matt Miller or Sailesh Gadia.

Contact the author:

Amy Matsuo
Principal and Leader
Regulatory and ESG Insights
amatsuo@kpmg.com